(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 670 036**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **91 14854**

(51) Int Cl[5] : G 06 F 13/38

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 29.11.91.

(30) **Priorité** : 30.11.90 JP 34042890.

(43) **Date de la mise à disposition du public de la demande** : 05.06.92 Bulletin 92/23.

(56) **Liste des documents cités dans le rapport de recherche** : *Le rapport de recherche n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s)** : *Société dite: KABUSHIKI KAISHA TOSHIBA* — JP.

(72) **Inventeur(s)** : Iijima Yasuo.

(73) **Titulaire(s)** :

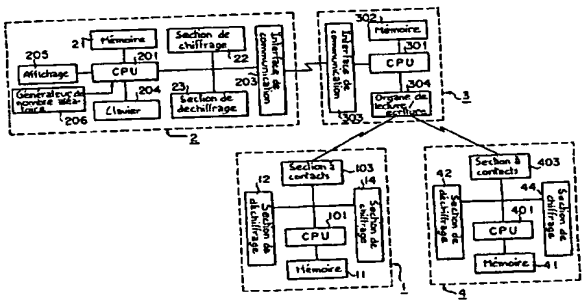
(74) **Mandataire** : Cabinet Beau de Loménie.

(54) Ensemble de communication de données.

(57) L'invention concerne un ensemble de communication de données.

Elle se rapporte à un ensemble destiné à faire communiquer un dispositif hôte (2) avec des cartes à circuit intégré (1, 4) par l'intermédiaire d'un terminal (3). Lorsqu'une session finale est exécutée entre le dispositif hôte (2) et une carte (1), des données de clé commune conservées dans le dispositif hôte sont chiffrées par une clé de session remise à jour et transmises à la carte (1) dans laquelle les données chiffrées de clé commune sont déchiffrées avec la clé remise à jour de session de manière que les données de clé commune soient obtenues pour les sessions à exécuter ultérieurement.

Application à la sécurité des communications entre des appareils électroniques.



FR 2 670 036 - A1

La présente invention concerne un ensemble de communication de données utilisant une clé de session dans une transaction exécutée par exemple entre un dispositif hôte et plusieurs cartes à circuit intégré.

Habituellement, dans un ensemble de communication de données comprenant un dispositif hôte, un terminal et analogue, les données ont d'abord été chiffrées à l'aide de données prédéterminées de clé (données de clé de session), et les données chiffrées ont ensuite été transmises afin que la sécurité des données soit accrue. Pour que la sécurité soit encore accrue, on a récemment proposé un procédé de chiffrage des données de clé de session et de transmission des données chiffrées de clé de session. Une clé d'une session précédente, qui a déjà été utilisée une fois, peut être utilisée en pratique à nouveau comme clé de chiffrage-déchiffrage pour la transmission des données actuelles de clé de session. Aucun problème ne se pose dans ce cas si deux appareils destinés à transmettre et recevoir les données sont fixes ou prédéterminés. Dans la transaction exécutée entre un dispositif hôte et plusieurs cartes à circuit intégré cependant, les clés finales de session des cartes respectives à circuit intégré doivent toutes être conservées du côté du dispositif hôte afin que les transactions soient satisfaisantes.

Un dispositif de mémoire destiné à conserver toutes les clés finales de session est nécessaire et constitue donc une charge croissante pour le dispositif hôte.

L'invention a donc pour objet la réalisation d'un ensemble de communication de données utilisant une clé de session et supprimant la charge d'un dispositif hôte.

L'invention concerne ainsi un ensemble de communication de données destiné à communiquer des données entre un premier et un second appareil électronique,

le premier appareil électronique comprenant :

une première mémoire destinée à conserver des données de clé commune,

un dispositif générateur de données de clé de session destiné à créer des données de clé de session pour chaque session,

un premier dispositif de chiffrage des données de clé de session à l'aide des données de clé commune, et

un premier dispositif de transmission des données chiffrées par le premier dispositif de chiffrage au second appareil électronique, et

le second appareil électronique comprenant :

une seconde mémoire destinée à conserver les données de clé commune,

un dispositif de déchiffrage des données chiffrées de clé de session, reçues du premier dispositif électronique, à l'aide des données de clé commune,

un second dispositif de chiffrage des secondes données de communication à transmettre au premier appareil électronique à l'aide des données de clé de session,

un second dispositif de transmission des secondes données de communication chiffrées par le second dispositif de chiffrage au premier appareil électronique, et

un dispositif de remise à jour des données de clé commune conservées dans la seconde mémoire par les données de clé de session déchiffrées par le dispositif de déchiffrage,

les données de clé créées par le dispositif générateur de données de clé étant transmises au second appareil électronique chaque fois qu'une session de données est réalisée entre le premier et le second appareil électronique.

Un dispositif hôte et un appareil électronique, par exemple des cartes à circuit intégré, mémorisent des données de clé d'une session prédéterminée, et les garde comme clé pour le chiffrage-déchiffrage des mêmes données de transmission obtenues dans des sessions respectives. Après la session finale, la clé de session est chiffrée et transmise par le dispositif hôte aux cartes à circuit

intégré à l'aide des données transmises et elle est déchiffrée et conservée du côté des cartes à circuit intégré.

D'autres caractéristiques et avantages de l'invention seront mieux compris à la lecture de la description qui va suivre d'exemples de réalisation, faite en référence aux dessins annexés sur lesquels :

les figures 1A et 1B sont des diagrammes synoptiques représentant ensemble la disposition d'un ensemble de communication de données dans un mode de réalisation de l'invention ;

la figure 2 est un diagramme synoptique représentant l'ensemble de communication de données des figures 1A et 1B ;

la figure 3 est un diagramme synoptique représentant plus précisément une mémoire utilisée dans l'ensemble de communication de données représenté sur la figure 2 ; et

la figure 4 est un diagramme synoptique d'un autre exemple de mémoire représenté sur la figure 3.

On décrit maintenant en détail, en référence aux dessins annexés, un mode de réalisation de l'invention dans lequel un ensemble de communication de données utilisant une clé de session s'applique à un ensemble comprenant un dispositif hôte, un terminal et des cartes à circuit intégré.

La disposition de l'ensemble de communication de données de ce mode de réalisation de l'invention est décrite dans la suite en référence à la figure 2. Un dispositif hôte 2 comprend une unité centrale de traitement CPU 201 destinée à commander les opérations des éléments constituant le dispositif hôte 2, une mémoire permanente 21 destinée à conserver divers types d'informations, notamment des programmes de commande de l'unité CPU 201, un circuit 203 d'interface de communication qui communique avec un terminal 3, un clavier 304 grâce auquel un utilisateur saisit des données, des instructions et analogues, un dispositif 205 d'affichage, par exemple un tube à rayons cathodiques destiné à afficher le résultat d'un calcul, des

données transmises ou analogues, un générateur 206 de nombre aléatoire destiné au chiffrage de données à transmettre, un module de chiffrage 22 (appelé section de chiffrage dans la suite) destiné à chiffrer les données à transmettre, et un module de déchiffrage 23 (appelé section de déchiffrage dans la suite) destiné à déchiffrer les données reçues.

Le terminal 3 comprend une unité CPU 301 destinée à commander les opérations des éléments constituant le terminal 3, une mémoire 302 destinée à conserver divers types d'informations, un circuit 303 d'interface de communication qui communique avec le dispositif hôte 2, et un appareil de lecture-écriture 304 destiné à lire-écrire des données échangées avec les cartes à circuit intégré 1 et 4.

Les cartes à circuit intégré 1 et 4 comportent des unités centrales de traitement CPU 101 et 401 destinées à commander les opérations des éléments constituant les cartes 1 et 4, des mémoires permanentes 11 et 41 destinées à conserver divers types d'informations, des parties de contact 103 et 403 destinées à connecter électriquement la carte 1 ou 4 à circuit intégré à l'appareil de lecture-écriture 304, des sections de chiffrage 14 et 44 destinées à chiffrer des données à transmettre, et des sections 12 et 42 de déchiffrage des données reçues respectivement.

La mémoire 11 de la carte 1 comprend une zone 11a de système et une zone 11b de données comme représenté sur la figure 3. La zone de système 11a peut être atteinte par l'unité centrale CPU 101 uniquement et elle contient un programme, et la zone de données 11b conserve des données résultant de transaction sous forme d'une mémoire de travail. La mémoire 41 de la carte 4 a la même structure et les mêmes fonctions que la mémoire 11 de la carte 1.

Les figures 1A et 1B représentent un ordinogramme du traitement des données dans le cas où des données conservées dans la mémoire 11 de la carte 1 sont lues par le terminal 3 et remises à jour par le dispositif hôte 2, et les données remises à jour sont transmises à la carte 1.

Dans l'ensemble de communication de données décrit précédemment, on détermine d'utiliser des données "XXX" comme clé de session de transmission. Dans le traitement de données représenté sur les figures 1A et 1B, la carte 1 est introduite dans l'appareil 304 de lecture-écriture du terminal 3 afin qu'elle communique avec le dispositif hôte 2. La carte 1 et le dispositif hôte 2 ont les mémoires permanentes 11 et 21 respectivement et une clé prédéterminée de session de transmission XXX est conservée dans ces mémoires 11, 21 dans la première étape, par exemple lorsqu'une carte 1 est expédiée par l'usine ou lorsque la carte 1 est délivrée à l'utilisateur d'une banque par exemple. La touche de session de transmission XXX est aussi mémorisée dans la mémoire permanente 41 de la carte 4.

Si la carte 1 est introduite dans l'appareil de lecture-écriture 304 du terminal 3 et peut communiquer avec le dispositif hôte 2 par le terminal 3, les données de clé de première session "clé 1" créées par le générateur 206 de nombre aléatoire placé dans le dispositif 2 hôte sont chiffrées par la section 22 de chiffrage à l'aide des données de clé de session de transmission "XXX" constituant une clé de chiffrage. Les données chiffrées de clé de session "clé 1'" sont transmises à la carte 1 par le terminal 3 et déchiffrées dans la section 12 de déchiffrage à l'aide des données de clé de session de transmission "XXX" qui sont lues dans la zone 11a du système de la mémoire 11, comme indiqué sur la figure 3, par l'unité centrale 101, si bien que la clé 1 des données de clé de la première session est extraite. Ensuite, la clé de session de transmission "XXX" conservée dans la zone du système 11a subit une réécriture sous forme "clé 1" de données de première session.

Lorsqu'une transaction est réalisée avec la carte 1, des données M1 conservées dans la zone de données 11b de la mémoire 11 de la carte 1 sont lues et transmises au dispositif hôte 2 avec des données d'identification de carte (ID) de la carte 1, conservées dans la zone du système 11a.

Les données M1 et l'identification de carte ID sont chiffrées dans la section 14 avec les données de clé de première session "clé 1" conservées dans la zone 11a du système de la mémoire 11 sous forme de clé de chiffrage, et les données chiffrées (M1+ID)'sont alors transmises au dispositif hôte 2. Comme décrit précédemment, dans la carte 1, les données (M1+ID)' chiffrées avec la "clé 1" des données de clé de première session reçues du dispositif hôte 2 sont transmises au dispositif hôte 2. Même si les données chiffrées sont reçues par un tiers, entre le terminal 3 et le dispositif hôte, le tiers, comme il ne dispose pas de la "clé 1" des données de clé de première session, ne peut pas déchiffrer les données. Les données (M1+ID)' sont déchiffrées avec la "clé 1" des données de clé de première session dans la section 23 de déchiffrage du dispositif hôte 2, et les données M1 et l'identité ID de la carte sont extraites. L'identité ID est comparée à des données d'identité enregistrées préalablement dans le dispositif hôte 2 pour la vérification de la carte 1. Lorsque celle-ci a été vérifiée, les données M1 sont calculées avec des données de transaction m1 saisies à l'aide du terminal 3 d'un point de vente par exemple, afin que des données remises à jour M2 soient obtenues. L'opération de la première session "session 1" est ainsi terminée.

Ensuite, l'opération de la seconde session "session 2" commence. La "clé 2" des données de clé de la seconde session créée à partir du générateur 206 de nombre aléatoire est chiffrée par la section de chiffrage 22 à l'aide de la "clé 1" des données de clé de la première session sous forme d'une clé de chiffrage, et la "clé 2'" des données chiffrées de clé de session est transmise à la carte 1. Dans la carte 1, la "clé 2'" des données chiffrées est déchiffrée dans la section 12 à l'aide de la "clé 1" des données de clé de la première session conservées dans la zone du système 11a sous forme d'une clé de déchiffrage, et la "clé 2" des données de clé de la seconde session est extraite. Ensuite, la "clé 1" des données de clé de la

première session conservées dans la zone du système 11a est réécrite sous forme de la "clé 2".

Les données M remises à jour dans le dispositif hôte 2 sont chiffrées dans la section de chiffrage 22 à l'aide de la "clé 2" des données de clé de seconde session. les données chiffrées et remises à jour M2' sont transmises à la carte 1 et déchiffrées dans la zone 12 de déchiffrage avec la "clé 2" des données de clé de seconde session lues dans la zone du système 11a. Dans la carte 1, les données remises à jour M2 sont conservées dans la zone de données 11b. L'opération de la seconde session est alors terminée. Comme décrit précédemment, les clés de session conservées dans la mémoire 11 de la carte à circuit intégré sont réécrites successivement à chaque session. Bien que les données chiffrées puissent être reçues par un tiers en cours de session, les données ne peuvent pas être déchiffrées si bien que la sécurité de la transaction est conservée.

Lorsque l'opération de la session suivante n'est pas réalisée dans la carte 1 à circuit intégré, la clé "XXX" de session de transmission est transmise par le dispositif hôte 2 à la carte 1, et le traitement de données est terminé. Si la fin de la session est détectée du côté du dispositif hôte 2, la clé "XXX" conservée dans la mémoire permanente 21 est lue et chiffrée dans la section de chiffrage 22 avec la "clé 2" des données de clé de seconde session sous forme de clé de chiffrage. Une clé "XXX'" de session chiffrée de transmission est transmise à la section de déchiffrage 12 de la carte 1 à circuit intégré. Les données peuvent être déchiffrées uniquement par la carte 1 dans laquelle la "clé 2" des données de clé de la seconde session, utilisée dans la seconde session antérieure, est conservée dans la zone du système 11a. La clé déchiffrée de session de transmission "XXX" est conservée dans la zone du système 11a de la mémoire 11 pour l'opération de la session suivante.

La troisième et la quatrième session (session 3 et session 4) entre le dispositif hôte 2 et la carte 4 sont maintenant décrites en référence à la figure 1B. Comme décrit précédemment, la touche de session de transmission "XXX" est conservée préalablement dans la zone du système de la mémoire permanente 41 de la carte 4. Si la carte 4 est introduite dans le terminal 3 et des données peuvent être reçues et émises entre le dispositif hôte 2 et une carte 4, une "clé 3" de données de clé de troisième session créée par le générateur 206 de nombre aléatoire est chiffrée par la clé "XXX" et est transmise à la section 42 de déchiffrage de la carte 4. La "clé 3" déchiffrée dans la zone du système de la mémoire 41 est utilisée comme clé pour le chiffrage des données M3 et de l'identité ID de la carte lue dans la zone de données de la mémoire 41. Les données M3 et le numéro d'identification ID de la carte sont chiffrés par la "clé 3" dans la section 44 de chiffrage puis transmises au dispositif hôte 2. Les données M3 sont calculées à l'aide des données de transaction m2 saisies par exemple à partir du terminal 3, et des données remises à jour, par exemple des données de nouveau solde M4, sont créées. L'opération de la troisième session est alors terminée.

L'opération de la quatrième session commence alors. Dans la quatrième session, la "clé 4" de quatrième session créée par le générateur 206 de nombre aléatoire est chiffrée dans la section 22 à l'aide de la "clé 3" de troisième session comme clé de chiffrage, et la "clé 4'" sous forme chiffrée est transmise à la carte 4. Dans la carte 4, la "clé 4'" est déchiffrée dans la section 42 avec la "clé 3" de la troisième session conservée dans la zone du système de la mémoire 41 comme clé de déchiffrage, et la "clé 4" de la quatrième session est extraite. La "clé 4" est conservée dans la zone du système de la mémoire 41 à la place de la "clé 3".

Les données M4 remises à jour par le dispositif hôte 2 sont chiffrées dans la section 22 à l'aide de la "clé 4",

et les données chiffrées M4' sont transmises à la carte 4 et sont déchiffrées dans celle-ci dans la section 42 à l'aide de la "clé 4" conservée dans la zone du système de la mémoire 41. L'opération de la quatrième session est alors terminée.

S'il se confirme que la session suivante n'est pas exécutée, la clé de session de transmission "XXX" est lue dans la mémoire 21 du dispositif hôte 2 et est chiffrée dans la section 22 de chiffrage à l'aide de la "clé 4". La clé chiffrée "XXX'" est transmise à la carte 4, puis déchiffrée dans la section 42 avec la "clé 4" et conservée dans la zone du système de la mémoire 41.

Dans le mode de réalisation précédent, comme l'indique la figure 3, les mémoires 11 et 41 des cartes 1 et 4 comprennent la zone du système 11a qui peut être atteinte par l'unité centrale de traitement CPU 101 ou 401 uniquement, et la zone de données 11b utilisée comme mémoire de travail. Cependant, l'invention n'est pas limitée à ces mémoires 11 et 41. Par exemple, comme l'indique la figure 4, les mémoires 11 et 41 peuvent être constituées afin qu'elles comprennent une mémoire morte effaçable et programmable électriquement 11A qui peut être atteinte par la seule unité centrale 101, et une mémoire à accès direct 11B utilisée comme mémoire de travail, respectivement.

Comme décrit précédemment, selon l'invention, un seul dispositif hôte constitue un ensemble connecté utilisant plusieurs cartes à circuit intégré et une clé de session commune aux cartes à circuit intégré et conservée dans les cartes respectives. En conséquence, la charge du dispositif hôte peut être largement réduite.

Bien entendu, diverses modifications peuvent être apportées par l'homme de l'art aux ensembles de communication de données qui viennent d'être décrits uniquement à titre d'exemples non limitatifs sans sortir du cadre de l'invention.

REVENDICATIONS

1. Ensemble de communication de données destiné à faire communiquer un premier et un second appareil électronique (2, 1) qui échangent des données, le premier et le second appareil électronique (2, 1) transmettant des premières et des secondes données, caractérisé en ce que :

le premier appareil électronique (2) comprend :

une première mémoire (21) destinée à conserver des données de clé commune,

un dispositif (206) générateur de données de clé de session destiné à créer des données de clé de session pour chaque session,

un premier dispositif (22) de chiffrage des données de clé de session avec les données de clé commune afin que des premières données chiffrées soient créées,

un premier dispositif (203) de transmission des premières données chiffrées par le premier dispositif de chiffrage au second appareil électronique (1), et

un premier dispositif (23) de déchiffrage de secondes données chiffrées qui sont des secondes données transmises par le second appareil électronique (1) et chiffrées avec les données de clé de session, et

le second appareil électronique (1) comprend :

une seconde mémoire (11) destinée à conserver les données de clé commune,

un dispositif (12) de déchiffrage des premières données chiffrées reçues du premier appareil électronique (2) à l'aide des données de clé commune afin que des données de clé de session soient obtenues,

un second dispositif de chiffrage (14) destiné à chiffrer les secondes données (2) à l'aide des données de clé de session de manière que les secondes données chiffrées, destinées à être transmises au premier dispositif électronique, soient créées,

un second dispositif (103) de transmission des secondes données chiffrées par le second dispositif de chiffrage (14) au premier appareil électronique (2), et

un dispositif (101) de remise à jour des données de clé commune conservées dans la seconde mémoire (11) par les données de clé de session déchiffrées par le second dispositif de chiffrage (12),

dans lequel les données de clé créées par le dispositif (206) générateur de données de clé sont transmises au second appareil électronique (1) chaque fois qu'une session de données est réalisée entre le premier et le second appareil électronique (2, 1).

2. Ensemble selon la revendication 1, caractérisé en ce qu'il comprend un dispositif (101) de remise à jour des données remises à jour de clé de session conservées dans la seconde mémoire (11) par utilisation des données de clé commune conservées dans la première mémoire (21) après la fin d'une session finale.

3. Ensemble selon la revendication 1, caractérisé en ce que le dispositif (206) générateur de données de clé de session comprend un générateur (206) de nombre aléatoire.

4. Ensemble selon la revendication 1, caractérisé en ce que le premier appareil électronique est un dispositif hôte (2), et le second appareil électronique (1) comporte plusieurs cartes à circuit intégré (1, 4).

5. Ensemble selon la revendication 1, caractérisé en ce que le second appareil électronique (1) comporte une unité centrale de traitement (101) destinée à commander le second appareil électronique (1), et la seconde mémoire (11) comprend une zone de mémoire (11b) accessible par l'unité centrale de traitement (101) uniquement.

6. Ensemble selon la revendication 1, caractérisé en ce que le second appareil électronique (1) comporte une unité centrale de traitement (101) destinée à commander le fonctionnement du second appareil électronique (1), et la seconde mémoire (11) comprend une mémoire morte effaçable et programmable électriquement (11A) accessible par l'unité centrale de traitement uniquement.

7. Ensemble de communication de données destiné à faire communiquer un premier et un second appareil

électronique (2, 1) afin qu'ils échangent des données, caractérisé en ce que :

le premier appareil électronique (2) comporte :

une première mémoire (21) destinée à conserver des données de clé commune,

un dispositif (206) générateur de données de clé de session destiné à créer des données de clé de session pour chaque session,

un premier dispositif (22) de chiffrage des données de clé de session avec les données de clé commune, et

un premier dispositif (203) destiné à transmettre des données chiffrées par le premier dispositif de chiffrage au second appareil électronique (1), et

le second appareil électronique (1) comporte :

une seconde mémoire (11) destinée à conserver les données de clé commune,

un dispositif (12) de déchiffrage des données chiffrées de clé de session reçues du premier appareil électronique (2) à l'aide des données de clé commune,

un second dispositif de chiffrage (14) destiné à chiffrer les secondes données de communication à transmettre au premier appareil électronique (2) à l'aide des données de clé de session,

un second dispositif (103) de transmission des secondes données de communication chiffrées par le second dispositif de chiffrage au premier appareil électronique (2), et

un dispositif (101) de remise à jour des données de clé commune conservées dans la seconde mémoire (11) par les données de clé de session déchiffrées par le second dispositif de déchiffrage (12),

les données de clé créées par le dispositif (206) générateur de données de clé étant transmises au second appareil électronique (1) chaque fois qu'une session de données est réalisée entre le premier et le second appareil électronique (2, 1).

8. Ensemble selon la revendication 7, caractérisé en ce que le premier appareil électronique (2) comprend :

un dispositif (22) de chiffrage des données de clé commune conservées dans la première mémoire (21) par utilisation des données de clé de session, et

un dispositif destiné à transmettre les données de clé commune chiffrées par le dispositif de chiffrage au second appareil électronique (1), lorsqu'une session finale entre le premier et le second appareil électronique (2, 1) est terminée.

9. Ensemble selon la revendication 8, caractérisé en ce que le second appareil électronique (1) comporte un dispositif (12) destiné à déchiffrer les données chiffrées de clé commune qui sont chiffrées et transmises par le premier appareil électronique (2) à l'aide des données de clé de session.

10. Ensemble selon la revendication 8, caractérisé en ce qu'il comprend un dispositif (101) de remise à jour des données remises à jour de clé de session conservées dans la seconde mémoire (11) par les données de clé commune déchiffrées par le dispositif de déchiffrage (12) après la fin d'une session finale.

11. Ensemble selon la revendication 7, caractérisé en ce que le dispositif générateur de données de clé de session comprend un générateur (206) de nombre aléatoire.

12. Ensemble selon la revendication 7, caractérisé en ce que le premier appareil électronique (2) est un dispositif hôte (2), et le second appareil électronique (1) comporte plusieurs cartes à circuit intégré (1, 4).

13. Ensemble selon la revendication 7, caractérisé en ce que le second appareil électronique (1) comporte une unité centrale de traitement (101) destinée à commander le second appareil électronique (1), et la seconde mémoire (11) comprend une zone (11b) de mémoire qui est accessible par l'unité centrale de traitement (101) uniquement.

14. Ensemble selon la revendication 7, caractérisé en ce que le second appareil électronique (1) comporte une

unité centrale de traitement (101) destinée à commander le fonctionnement du second appareil électronique (1), et la seconde mémoire (11) comprend une mémoire morte effaçable et programmable électriquement (11A) accessible par l'unité centrale de traitement (101) uniquement.

15. Ensemble selon la revendication 7, caractérisé en ce que le premier appareil électronique (2) comporte un second dispositif (23) de déchiffrage des secondes données de communication à l'aide des données de touche de session, les secondes données de communication étant chiffrées par le second dispositif de chiffrage (14) et transmises par le second appareil électronique (1).

16. Ensemble de communication de données destiné à faire communiquer un premier et un second appareil électronique (2, 1) qui échangent des données, ledit ensemble étant caractérisé en ce que :

le premier appareil électronique (2) comprend :

une première mémoire (21) destinée à conserver des données de clé commune,

un dispositif (206) générateur de données de clé de session destiné à créer des données de clé pour chaque session,

un premier dispositif (22) de chiffrage des données de clé commune conservées dans la première mémoire (21) par utilisation des données de clé de session,

un second dispositif (22) de chiffrage des données de clé de session avec les données de clé commune,

un premier dispositif (203) de transmission des données chiffrées par le second dispositif de chiffrage (22) au second appareil électronique (1), et

un second dispositif (203) de transmission des données de clé commune chiffrées par le premier dispositif de chiffrage (22), au second appareil électronique (1) lorsqu'une session finale est terminée entre le premier et le second appareil (2, 1), et

le second appareil électronique (1) comporte :

une seconde mémoire (11) destinée à conserver les données de clé commune,

un premier dispositif (12) de déchiffrage des données chiffrées de clé de session reçues du premier appareil électronique (2) à l'aide des données de clé commune,

un second dispositif (12) de déchiffrage des données chiffrées de clé commune chiffrées et transmises par le premier appareil électronique (2), à l'aide des données de clé de session,

un troisième dispositif (14) de chiffrage de secondes données de communication destinées à être transmises au premier appareil électronique (2), à l'aide des données de clé de session,

un troisième dispositif (103) de transmission des secondes données de communication chiffrées par le troisième dispositif de chiffrage (14) au premier appareil électronique (2),

un premier dispositif (101) de remise à jour des données de clé commune conservées dans la seconde mémoire (11) par les données de clé de session déchiffrées par le second dispositif de déchiffrage (12), et

un second dispositif (101) de remise à jour des données remises à jour de clé de session conservées dans la seconde mémoire (11) par les données de clé commune déchiffrées par le second dispositif (12) de déchiffrage après la fin de la session finale.

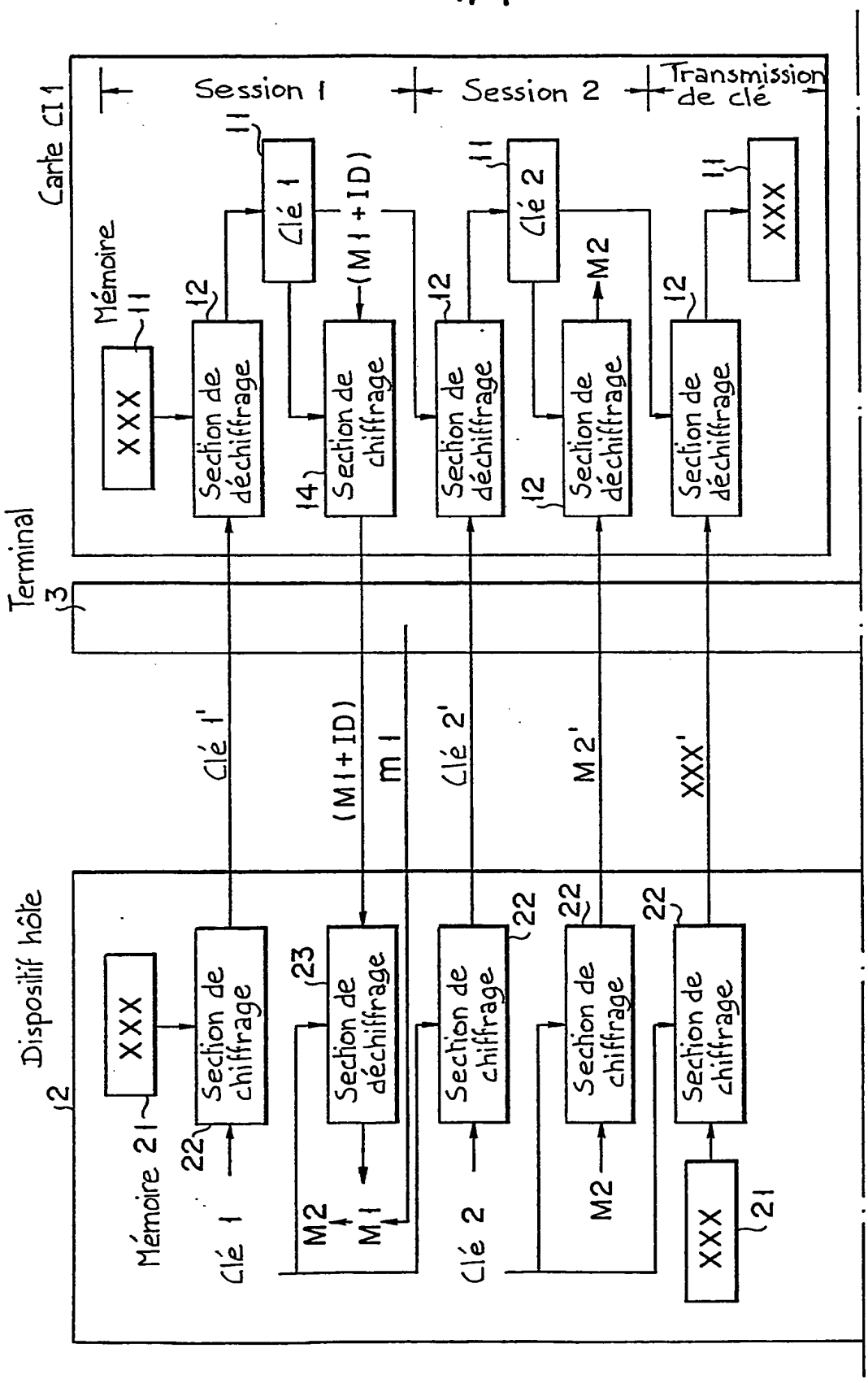

Carte CI 1
Session 1
Session 2
Transmission de clé
Mémoire
11
XXX
12
Section de déchiffrage
Clé 1
(M1 + ID)
14
Section de chiffrage
Clé 2
M2
XXX
Terminal
3
Clé 1'
(M1+ID)
M1
Clé 2'
M2'
XXX'
Dispositif hôte
2
Mémoire 21
XXX
22
Section de chiffrage
Clé 1
23
Section de déchiffrage
M2
M1
Clé 2
M2
XXX
21

FIG. 1A

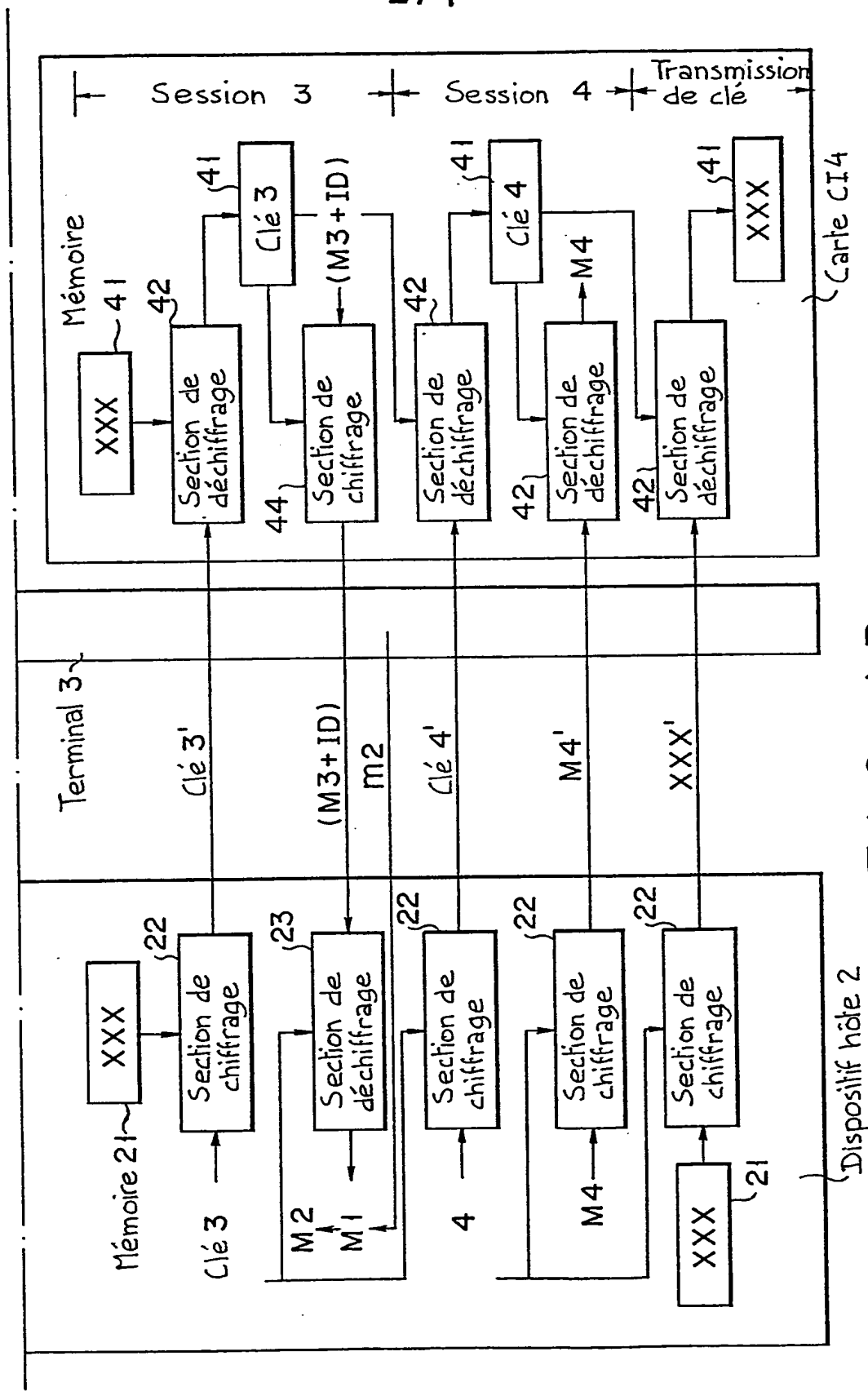

Session 3
Session 4
Transmission de clé
Mémoire
41
42
XXX
Section de déchiffrage
Clé 3
Clé 4
XXX
(M3+ID)
M4
44
Section de chiffrage
Carte CI4
Terminal 3
Clé 3'
(M3+ID)
m2
Clé 4'
M4'
XXX'
22
23
Section de chiffrage
Section de déchiffrage
Mémoire 21
M2
M1
4
21
Dispositif hôte 2

FIG. 1B

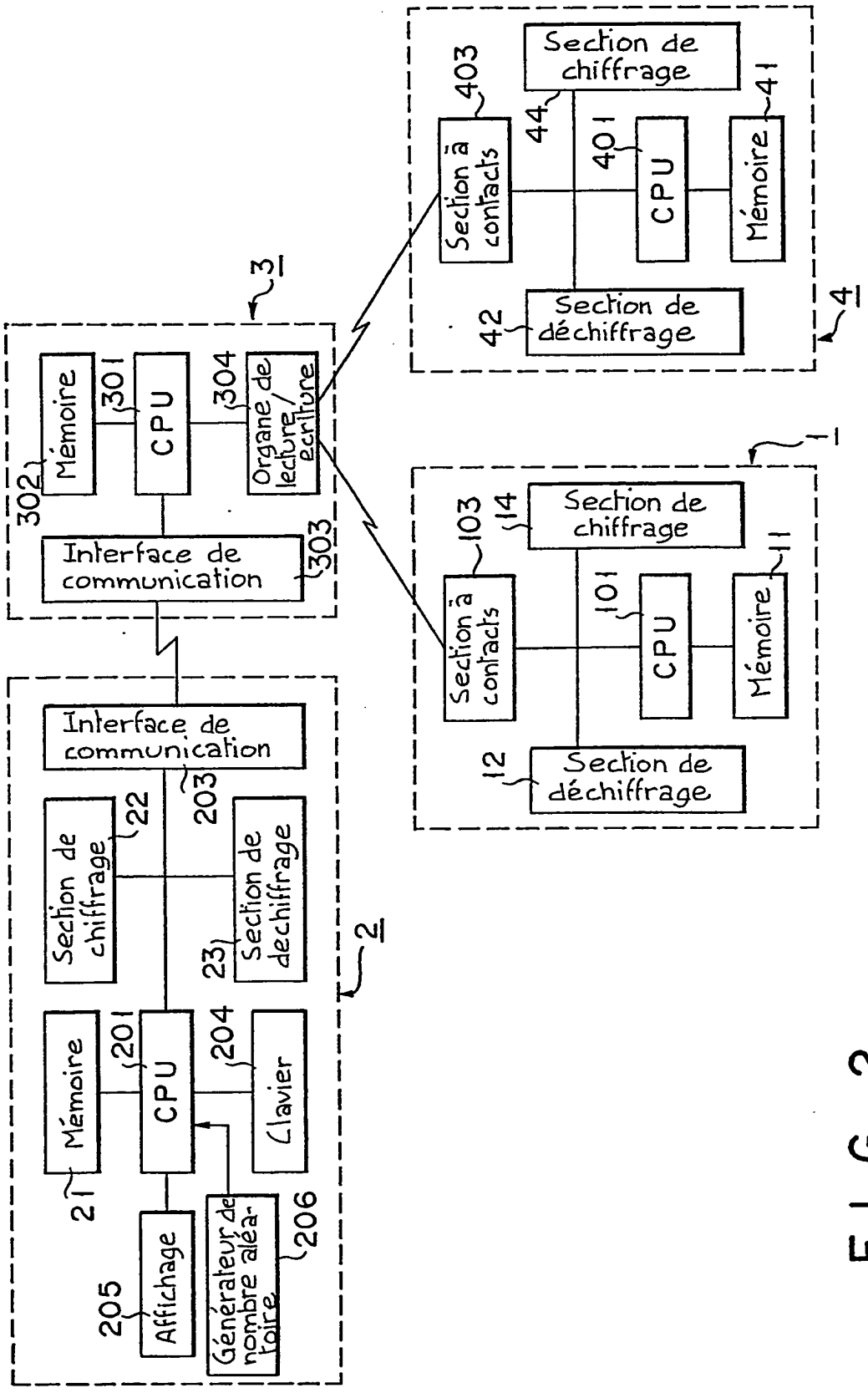

Section de chiffrage
403
44
401
41
Section à contacts
CPU
Mémoire
Section de déchiffrage
42
4
3
Mémoire
301
CPU
304
Organe de lecture/écriture
302
Interface de communication
303
1
103
14
Section de chiffrage
Section à contacts
101
CPU
11
Mémoire
12
Section de déchiffrage
Interface de communication
203
22
Section de chiffrage
Section de déchiffrage
23
2
Mémoire
201
CPU
204
Clavier
21
205
Affichage
206
Générateur de nombre aléatoire

FIG. 2

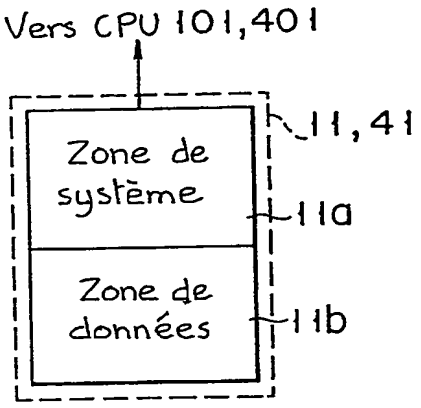

Vers CPU 101,401
11,41
Zone de système
11a
Zone de données
11b

FIG. 3

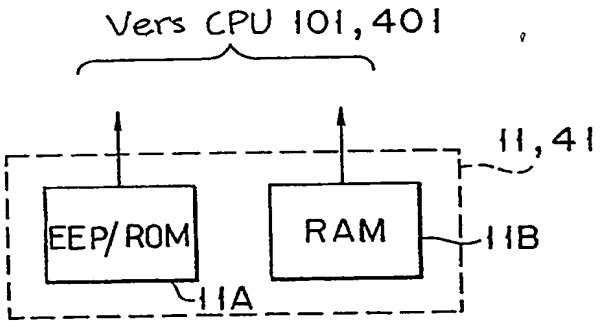

Vers CPU 101,401
11,41
EEP/ROM
RAM
11B
11A

FIG. 4